IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

VERONICA JOAQUIN-TORRES, individually and on behalf of all others similarly situated,	)	**Case No.:**
Plaintiff,	)	
v.	)	**CLASS ACTION COMPLAINT**
NELNET SERVICING, LLC	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Veronica Joaquin-Torres ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Nelnet Servicing, LLC ("Nelnet" or "Defendant"). Based upon personal knowledge as well as information and belief, Plaintiff specifically alleges as follows:

NATURE OF THE ACTION

1. This is a class action for damages against Nelnet Servicing, LLC, for its failure to exercise reasonable care in securing and safeguarding the sensitive personal data of student loan borrowers— including names, email addresses, phone numbers, and Social Security numbers, collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of student loan borrowers whose sensitive PII was stolen by cybercriminals in a cyber-attack beginning on or around June 1, 2022 and not ending until July 22, 2022 (the "Data Breach").

3. The Data Breach affected at least 2,501,324 individuals from Nelnet services.

4. Nelnet has notified Plaintiff that the information compromised in the Data Breach included her PII.

5. Plaintiff was not notified of the Breach until the end of August 2022, approximately three months after her Private Information was first accessed.

6. As a result of the Data Breach, Plaintiff has experienced various types of misuse of her PII, including a fraudulent credit card application in her name.

7. There has been no assurance offered from Nelnet that all personal data or copies of data have been recovered or destroyed. Nelnet offered Experian credit monitoring, which does not guarantee security of Plaintiff's information.

8. Accordingly, Plaintiff asserts claims for violations of negligence, an intrusion upon seclusion, breach of implied contract, breach of fiduciary duty, breach of Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq*., and a violation of the Nebraska Uniform Deceptive Trade Practices Act ("UDTPA"), Nebraska Revised Statutes §§ 87-301, *et. seq*.

PARTIES

A. Plaintiff Veronica Joaquin-Torres

9. Plaintiff Veronica Joaquin-Torres is a resident of North Carolina and brings this action in her individual capacity and on behalf of all others similarly situated. Plaintiff has been a student since 2016 and has taken out loans to fund her education. Oklahoma Student Loan Authority ("OSLA"), Joaquin-Torres's loan servicer, contracts with Nelnet to provide its servicing system and customer website portal. As part of this, Nelnet was entrusted with Joaquin-Torres's PII. On or around August 31, 2022, Joaquin-Torres received a notification letter from OSLA stating that her PII was taken from Nelnet's systems. The stolen PII included Joaquin-

Torres's name, address, email address, phone number, and Social Security number. The letter also advised Joaquin-Torres to contact the Federal Trade Commission.

10. The letter also offered 24 months of credit monitoring through Experian, which was ineffective for Joaquin-Torres and Class members. The credit monitoring would have shared her information with third parties and could not guarantee complete privacy of her sensitive PII.

11. A malicious actor has already applied for a credit card using Joaquin-Torres's name and previous address, PII that was stolen in the breach.

12. Other harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through malicious use of Joaquin-Torres's and other Class members' stolen Information.

B. Defendant

13. Defendant Nelnet Servicing, LLC is a Lincoln, Nebraska based student loan servicing company, which has a principal place of business at 121 S. 13th Street, Suite 100, Lincoln, Nebraska, 6850.

14. Defendant provides a technical servicing system and customer website portal for the Oklahoma Student Loans Authority, a student loan servicer, and/or other student loan servicing entities.

15. Defendant is a wholly owned subsidiary of Nelnet Diversified Solutions LLC, a Lincoln, Nebraska based limited liability company, which is itself a wholly owned subsidiary of Nelnet Inc., a Lincoln, Nebraska based corporate conglomerate that deals in the administration and repayment of student loans and education financial services.

16. As of March 31, 2022, Nelnet Inc. and/or its subsidiaries serviced $556.7 billion in loans for approximately 16.8 million borrowers. [1]

17. All of Plaintiff's claims stated herein are asserted against Nelnet and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

18. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

14. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(1), because Defendant maintains its principal place of business in this District and therefore is a resident in this District pursuant to 28 U.S.C. § 1391(c)(2).

FACTS

16. On or about July 21, 2022, Defendant informed its corporate customer OSLA that it had discovered an unauthorized user accessed its network. Nelnet's network contained student borrowers' Private Information including names, addresses, email addresses, phone numbers, and Social Security Numbers.

[1] Nelnet, Inc., *Nelnet Releases First Quarter 2022 Results*, NELNETINVESTORS.COM, https://www.nelnetinvestors.com/news/press-release-details/2022/Nelnet-Reports-First-Quarter-2022-Results/default.aspx

17. After it learned of the Data Breach, Nelnet investigated. As a result of the Data Breach, Defendant initially estimated that the breach included the PII of 2,501,324 student borrowers and/or other individuals.

18. Nelnet began notifying state Attorneys General and Class members about this widespread breach on August 26, 2022, over a full month after it had notified its corporate customers.

19. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected student borrowers, which resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

20. Nelnet's notice of the Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its systems, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was a system-wide breach, whether servers storing information were accessed, and how many student borrowers were affected by the Data Breach. Even worse, Nelnet offered only twenty-four months of identity monitoring to Plaintiff and Class members, an offer requiring disclosure of additional PII that Nelnet had just demonstrated it could not be trusted with.

21. Plaintiff and Class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and Class members' unencrypted, unredacted information, including names, addresses, email addresses, dates of birth, Social Security Numbers, and more.

22. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the financial industry, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

23. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was compromised through unauthorized access by an unknown third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Nelnet's Privacy Promises

24. Nelnet has made, and continues to make, various promises to student borrowers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

25. In its Notice of Data Breach letter to the victims of the Data Breach, Nelnet claims that it takes the privacy and security of your information very seriously, stating, "The confidentiality, privacy, and security of our customers' information is one of our highest priorities."

26. Defendant's Privacy Policy ("Privacy Policy") states "Protecting your privacy is important to Nelnet and our employees ... We implement reasonable and appropriate physical,

procedural, and electronic safeguards to protect your information."[2]

27. Defendant's Privacy Policy applies to any personal information provided to Nelnet and any personal information that Nelnet collects from its website, affiliates, and mobile apps.[3]

28. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiff and Class members' Private Information unless complying with laws or to carry out internal functions. [4]

29. The Privacy Policy further states:

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection. [5]

30. By failing to protect Plaintiff and Class members' Private Information, and by allowing the Data Breach to occur, Nelnet broke these promises to Plaintiff and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customers' Private Information

31. Nelnet acquires, collects, and stores a massive amount of student borrowers' protected PII, including Social Security Numbers and other personally identifiable data.

32. As a condition of managing their student loans, or of allowing them to access

[2] *Nelnet Privacy Policy Mission* Statement, https://www.nelnet.com/privacy-and-security (last visited Sept. 9, 2022)

[3] *Id*

[4] *Id.*

[5] *Id.*

information about their student loans through an online portal, Nelnet requires that these borrowers entrust them with highly confidential Private Information.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, Nelnet assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class members' Private Information from disclosure.

34. Defendant had obligations created by industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Defendant failed to properly safeguard Class members' Private Information, allowing unauthorized actors to access their Private Information.

36. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

37. Plaintiff and the Class members, as current or former student loan borrowers, reasonably relied on this sophisticated student loan servicing company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Borrowers, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

38. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

39. Defendant's failure to provide adequate security measures to safeguard

customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

40. In fact, Defendant has been on notice for years that Plaintiff and Class members' PII was a target for malicious actors. Despite such knowledge, Nelnet failed to implement and maintain reasonable and appropriate security measures to protect Plaintiff and Class members' PII from unauthorized access it should have anticipated and guarded against.

41. Defendant was also on notice that the federal government has been concerned about data security. In 2021, the FTC updated its consumer information Safeguards Rule, requiring non-banking financial institutions such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain comprehensive security systems to keep their customer's information safe. Against the backdrop of a rapid increase in cybersecurity incidents related to consumer financial information, Samuel Levine, the director of the FTC's Bureau of Consumer Protection The warning stated that "Financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it."[6]

42. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[7] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[8] That trend continues.

[6] *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data

[7] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[8] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

43. The average time to identify and contain a data breach is 287 days,[9] with some breaches going unrecognized for months leading to costly recover efforts and financial impact. Additionally, the median cost per US consumer incurred on each fraud-related data breach incident in 2020 was $450.[10] Data breaches and identity theft have a crippling effect on individuals and detrimental impact on the economy as a whole.[11]

44. A 2021 study conducted by Verizon showed that internal mismanagement of data security, including mis-delivery of emails, represents nearly 44 percent of the data breaches in the financial sector.[12] The majority of these incidents involve the sending or releasing of information to unauthorized actors.[13]

45. Almost half of the data breaches globally are caused by internal errors, either human mismanagement of sensitive information, or system errors.[14] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[15] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[16]

[9] IBM SECURITY, COST OF A DATA BREACH REPORT 6 (2021) [hereinafter COST OF A DATA BREACH REPORT]

[10] Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime* (2020), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#top

[11] *Id.*

[12] *Financial and Insurance Data Breaches*, VERIZON 2021 DIBR DATA BREACH SURVEY (2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/.

[13] *Id.*

[14] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

[15] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

[16] *Id.*

46. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[17]

47. To prevent and detect unauthorized access, including the systems changes that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary

[17] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

48. To prevent and detect unauthorized access to its systems, including the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[18]

49. To prevent the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
- Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
- use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

- **Harden infrastructure**
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

[18] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.
[19] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-

50. These are basic, common-sense email security measures that every business, not only those who handle sensitive personal information, should be doing. Nelnet, as a sophisticated manager of millions of student loans, should have been doing even more. But by adequately taking these common-sense solutions, Nelnet could have prevented this Data Breach from occurring.

51. Charged with handling sensitive PII, Nelnet knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on student borrowers as a result of a breach. Nelnet failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

52. With respect to training, Nelnet specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

53. The PII was also maintained on Nelnet's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's negligently maintained systems. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiff and Class members' PII was a known risk to Nelnet, and Nelnet was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

disaster/.

C. The Monetary Value of Privacy Protections and Private Information

54. The fact that Plaintiff and Class members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

55. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiff and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

56. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[20] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive consumer information on multiple underground Internet websites, commonly referred to as the dark web.

57. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

[20] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[21] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

58. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[22]

59. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[23]

60. Recognizing the high value that consumers place on their Private Information, many companies now offer individual consumers an opportunity to sell this information.[24] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

61. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value

[22] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274 [hereinafter *Web's New Hot Commodity*].

[23] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[24] *Web's Hot New Commodity*, *supra* note 22.

their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[25]

62. The ramifications of Nelnet's failure to keep student borrowers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

63. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[26] This gives thieves ample time to make multiple fraudulent purchases under the victim's name.

64. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the financial industry and related industries

65. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the phishing attack into their systems and, ultimately, the theft of their customers' Private Information.

66. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an

[25] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[26] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[27] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[28] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class members that was misused.

67. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

68. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

[27] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[28] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

69. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

70. Acknowledging the damage to Plaintiff and Class members, Defendant instructed customers like Plaintiff to "remain vigilant for instances of identity theft and fraud over the next 24 months." Plaintiff and the other Class members now face a greater risk of identity theft.

71. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. Nelnet Failed to Comply with FTC Guidelines

72. Nelnet was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

[29] *Start With Security: A Guide for Business*, FED. TRADE. COMM'M (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

74. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[30] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

75. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[31]

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. Nelnet failed to properly implement basic data security practices. Nelnet's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[30] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[31] *Start with Security*, *supra* note 31.

78. Nelnet was at all times fully aware of its obligation to protect the Private Information of customers because of its position as a trusted student loans services provider. Nelnet was also aware of the significant repercussions that would result from its failure to do so.

E. Damages to Plaintiff and the Class

79. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

80. The ramifications of Nelnet's failure to keep customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[32]

81. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

82. Defendant further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

83. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff and Class

[32] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

members' Private Information as detailed above, and Plaintiff is now at a heightened and increased risk of identity theft and fraud.

84. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

85. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, services billed in their name, and similar identity theft.

86. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

87. Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with Nelnet. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

88. Plaintiff and Class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

89. Plaintiff and members of the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

90. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[33] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[34] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[35]

91. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[36]

92. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the insurance context, Private Information can be used to submit false

[33] *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

[34] *Id.*

[35] *Id.*

[36] *Id.*

insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

93. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

94. The Private Information belonging to Plaintiff and Class members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

95. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff and Class members' Private Information

from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

96. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

97. Defendant did not properly train their employees to identify and avoid phishing attempts.

98. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff and Class members' Private Information.

99. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

100. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[37]

101. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiff and Class members other than telling them to simply do the following:

- "remain vigilant for incidents of fraud and identity theft";
- "review[] account statements and monitor[] your credit report for unauthorized activity";
- obtain a copy of free credit reports;

[37] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff and Class members' Private Information.

102. Defendant's failure to adequately protect Plaintiff and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Nelnet's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class members to discover possible fraudulent activity and identity theft.

103. While Defendant offered twenty-four month of credit monitoring, Plaintiff could not trust a company that had already breached her data. The credit monitoring offered from Experian does not guarantee privacy or data security for Plaintiff who would have to expose her information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts. For example, Plaintiff caught a fraudulent credit card opened in her name. Were it not for her promptness, her credit score, reputation, and finances could have been affected by debts incurred in her name.

104. Moreover, the offer of 24 months of identity monitoring to Plaintiff and Class members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity

monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[38]

105. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and Class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

106. The Private Information stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

[38] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

107. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

e. Current and future costs in terms of time, effort and money that will beexpended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and

f. Anxiety and distress resulting fear of misuse of their Private Information.

108. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

109. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

110. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

111. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Nationwide Class and North Carolina Subclass:

> **Nationwide Class**
>
> All persons whose Private Information was compromised as a result of the Data Breach discovered on or about June of 2022 and who were sent notice of the Data Breach.
>
> **North Carolina Subclass**
>
> All persons residing in North Carolina whose Private Information was compromised as a result of the Data Breach discovered on or about June of 2022 and who were sent notice of the Data Breach

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

112. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

113. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class number in the millions.

114. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

h. Whether Defendant was unjustly enriched by its actions; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

115. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual

questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

116. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

117. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because her interests do not conflict with the interests of the Classes she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

118. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

119. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for

inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, the North Carolina Subclass)

120. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

121. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

122. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

123. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

124. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

125. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the financial industry.

126. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff and Class members' Private Information.

127. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

128. Because Defendant knew that a breach of their systems would damage thousands of its customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

129. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by

laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

130. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

131. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

132. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

133. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff and Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Plaintiff and Class members' Private Information;

d. Failing to detect in a timely manner that Plaintiff and Class members' Private Information had been compromised; and

e. Failing to timely notify Plaintiff and Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

134. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff and Class members' Private Information during the time it was within Defendant's possession or control.

135. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

136. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

137. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

138. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and the Nationwide Class, or alternatively, the North Carolina Subclass)

139. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

140. Plaintiff and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide loan servicing and, impliedly, if not explicitly, agreed to protect Plaintiff and Class members' Private Information.

141. These contracts include the privacy policy on Defendant's website.

142. To the extent Defendant's obligation to protect Plaintiff and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff and Class members' Private Information, including in accordance with federal, state and local laws; and industry standards. Plaintiff and Class members would not have entered into these contracts with Defendant without the understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

143. A meeting of the minds occurred, as Plaintiff and Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

144. The protection of Plaintiff and Class members' Private Information were material aspects of Plaintiff and Class members' contracts with Defendant.

145. Defendant's promises and representations described above relating to

industry practices, and about Defendant's purported concern about their clients' privacy rights became terms of the contracts between Defendant and their clients, including Plaintiff and Class members. Defendant breached these promises by failing to comply with federal law and reasonable industry practices.

146. Plaintiff and Class members read, reviewed, and/or relied on statements made by or provided by Nelnet and/or otherwise understood that Nelnet would protect its customers' Private Information if that information were provided to Nelnet.

147. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

148. As a result of Defendant's breach of these terms, Plaintiff and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure loan services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

149. Plaintiff and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, the North Carolina Subclass)

150. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

151. Plaintiff brings this breach of implied contract claim in the alternative to her breach of express contract claim.

152. Through their course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of loan servicing, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class members' Private Information.

153. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into the loan servicing agreement with Defendant.

154. The valid and enforceable implied contracts to provide loan services that Plaintiff and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

155. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

156. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

157. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

158. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

159. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide loan services to Plaintiff and Class members; and (b) protect Plaintiff and the Class members' Private Information provided to obtain loan services. In exchange, Plaintiff and members of the Class agreed to pay money for these services, and to turn over their Private Information.

160. Both the provision of services and the protection of Plaintiff and Class members' Private Information were material aspects of these implied contracts.

161. The implied contracts for the provision of loan services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class members' Private Information- are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

162. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff and Class members' Private Information.

163. Individuals who take out student loans value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining those loans

private. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

164. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant and/or its affiliated entities, and paid for the provided services, amongst other things, both the provision of services and the protection of their Private Information.

165. Plaintiff and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

166. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

167. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff and Class members' Private Information as set forth above.

168. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

169. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class members therefore were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

170. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have done business with Defendant and/or its affiliated providers.

171. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

172. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

173. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV
Breach of Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq*.,
(On Behalf of Plaintiff and the Nationwide Class)

174. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

175. Plaintiff, Class members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Consumer Protection Act ("CPA"), Neb. Rev. Stat. § 59-1601, et seq.

176. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

177. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

178. In addition, Defendant's failure to secure consumers' Private Information violated the FTCA and therefore violates the CPA.

179. Also, Defendant's failure to give timely notice of this Data Breach in violation of Nebraska's notification of security breach statute, Neb. Rev. Stat. § 87-801 et seq is an unfair or deceptive act pursuant to Neb. Rev. Stat. § 87-808, and therefore violates the Consumer Protection Act.

180. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

181. The aforesaid conduct constitutes a violation of the CPA, Neb. Rev. Stat. § 59-1603, in that it is a restraint on trade or commerce.

182. These violations have caused financial injury to the Plaintiff and the other Class members.

183. Defendant's violations of the CPA have an impact of great and general importance on the public, including Nebraskans. Tens of thousands of Nebraskans have been insured by Nelnet, an appreciable number of whom have been impacted by the Data Breach. In addition, Nebraska residents have a strong interest in regulating the conduct of its corporate citizens such as Nelnet, whose policies and practices described herein affected tens of thousands across the country.

184. As a direct and proximate result of Defendant's violation of the CPA, Plaintiff and Class members are entitled to a judgment under Neb. Rev. Stat. § 59-1609 to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

COUNT V
DECLARATORY RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

185. Plaintiff fully incorporates by reference all of the above paragraphs as though fully set forth herein.

186. Under the Declaratory Judgment Act, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

187. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff and Class members' Private Information, and whether Defendant is currently

maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

188. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumer Private Information.

189. Defendant still possesses the Private Information of Plaintiff and the Class.

190. Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

191. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

192. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Nelnet. The risk of another such breach is real, immediate, and substantial.

193. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Nelnet, Plaintiff and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

194. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Nelnet, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other customers whose Private Information would be further compromised.

195. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Nelnet implement and maintain reasonable security measures, including but not limited to the following:

196. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Nelnet's systems on a periodic basis, and ordering Nelnet to promptly correct any problems or issues detected by such third-party security auditors;

197. engaging third-party security auditors and internal personnel to run automated security monitoring;

198. auditing, testing, and training its security personnel regarding any new or modified procedures;

199. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

200. conducting regular database scans and security checks; and

201. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety; to disclose with specificity the type of PII compromised during the Data Breach; and to routinely and continually conduct training to inform internal security personnel how to prevent, identify, and contain a breach, and how to appropriately respond;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

Date: September 9, 2022 Respectfully submitted,

/s/ Jason S. Rathod
Jason S. Rathod*
jrathod@classlawdc.com
Nicholas A. Migliaccio*
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

*Permanently Admitted to Practice in D. Neb.